# Hilton Settles NY and VT State AG Investigation into 2015 Data Breach; Pays $700,000 Civil Penalty

Alyssa Z. Hutnik

November 2, 2017

New York Attorney General Eric T. Schneiderman and Vermont Attorney General TJ Donovan ("Attorneys General") announced a settlement with Hilton Domestic Operating Company, Inc. ("Hilton") resolving allegations that the company did not have reasonable data security practices in place and failed to provide timely notice after two security breaches involving payment card information. The settlement provides some valuable lessons to companies about the "most expedient time possible and without unreasonable delay" standard in state data breach laws, and how a data breach can uncover potentially deficient security standards that can raise exposure for companies.

**Timely Notice.** According to the Attorneys General, Hilton had sufficient information to trigger consumer and regulator notice well before Hilton's November 24, 2015 substitute notification. As indicated in the settlement, Hilton first learned of the initial data breach on February 10, 2015, and the second data breach on July 10, 2015. The company engaged a Private Forensic Investigator ("PFI"), who issued a preliminary incident response report for the first and second incident on March 10, 2015, and August 16, 2015, respectively. Hilton provided notice to consumers and regulators on November 24, 2015, more than 287 days after receiving notice of the first incident and 100 days after receiving notice of the second incident.

New York's breach notification law requires consumer notification in the "most expedient time possible and without reasonable delay." Vermont's breach notification law has the same standard for consumer notice, but also requires that notice be "no later than 45 days after discovery or notification, consistent with…any measures necessary to determine the scope of the security breach…." Under Vermont's breach notification law, a data collector must provide notice to the Attorney General within 14 days. According to the Attorneys General, and based on these laws, Hilton did not provide timely notice.

**Reasonable Data Security Practices**. The PFI's final incident report found that Hilton was not in compliance with Payment Card Industry Data Security Standard ("PCI DSS") requirements. The Vermont Attorney General alleged that this failure to maintain reasonable data security practices violated Vermont's Consumer Protection Act. The New York Attorney General noted that Hilton's website privacy policy and other online statements represented to consumers that Hilton would take reasonable measures to process personal information and that customers' information was safe. The New York Attorney General alleged that Hilton failed to honor these promises and, in so doing, violated New York's Executive Law and General Business Law, which prohibits deceptive acts or

practices in conducting business.

**Settlement Terms**. In addition to civil penalties totaling $700,000 ($300,000 for Vermont and $400,000 for New York), Hilton must:

- Provide notice to consumers affected by a breach in compliance with relevant state law.
- Send the Vermont Attorney General, for five years, all PFI preliminary reports on breaches involving cardholder data.
- Design, implement, and maintain a written comprehensive information security program.
- Annually obtain a written assessment of its compliance with PCI DSS and notify the Attorneys General of any PCI DSS assessment where the assessor does not find Hilton fully compliant.

As was the case here, the cost of a data breach is not limited to civil penalties but potentially includes ongoing settlement term compliance costs, intensive regulatory oversight, as well as reputational damage. And a delayed data breach notice can exacerbate the data breach exposure. This settlement is the latest reminder on how data breach preparedness – including a current incident response policy that is followed by the company – can help contain this type of fall-out.